APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/706,728	11/07/2000	Patrick Le Quere	T2147-906625	8212

181	7590	11/30/2005

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 11/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/706,728	LE QUERE, PATRICK
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 September 2005</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>15-34</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>15-34</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>07 November 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)   4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .   6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1.   In response to communications filed on 9/9/2005, applicant amends claims 15, 17, 18, 24,

29, and 30. The following claims 14-34 are presented for examination.

1. 1   In response to communications filed on 9/9/2005, applicant has overcome the objection

to the specification and the objection has been withdrawn.

1.2   Applicant's remarks, pages 9-10, filed on 9/9/2005, with respect to the rejection of claims

15-34 have been fully considered but they are not persuasive. Regarding claim 15, Applicant has

amended claim 15 to recite an input/output module "including a microcontroller and memory".

Examiner asserts that claim 45 as amended is still rendered obvious over Dyke and Bakhle either

alone or in combination. For instance, Dyke discloses a first input/output portion interfacing

with the host computer that meets the recitation of input/output module including microcontroller

and memory (see column 3, lines 55-65 and figure 1). Bakhle discloses an input/output module

including microcontroller and memory (figure 1) that also meets the recited input/output module

"including a microcontroller and memory" as stated in the last Office Action. Upon further

consideration Examiner maintains the rejection of claims 15-34 in view of the same references.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

Claims 15 and the intervening claims are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 15 is rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention. The amended claim recited the isolation means ... allows parallel operation of the input/output module and the encryption module" does not equate with the specification stating the isolation means "ensuring the parallelism of the operations performed by the input/output module and the encryption module".

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1   **Claims 15-17 and 29-32** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,063,596 to **Dyke** in view of US Patent 6,021,201 to **Bakhle et al.**

3.2   **As per claims 15-17, Dyke** discloses an encryption circuit (1) for simultaneously

processing various encryption algorithms, the encryption circuit adapted to be coupled with a

host computer system, characterized in that the circuit comprising: an input/output module

including a microcontroller and memory, that handles data exchanges between the host system

and the circuit via a dedicated bus, for example (see column 3, lines 55-65 and figure 1); an

encryption module coupled with the input/output module said encryption module controlling

encryption and decryption operations, as well as storage of all sensitive information of the

circuit, for example (see column 4, line 65 through column 4, line 8); and isolation means

comprising of a dual-port memory between the input/output module and the encryption module,

for making the sensitive information stored in the encryption module inaccessible to the host

system and for allowing parallel operation of the input/output module and the encryption

module, for example (see column 4, lines 24-40 and column 2, lines 30-53). **Dyke** discloses a

dual-port memory coupled with an input/output module and an encryption module performing

parallel processing and a dual-port memory being coupled to a first bus and adapted to

simultaneously handle the exchange of data, commands and statuses between the input/output

and encryption modules and providing means of isolating the input/output module and the

encryption module (see also column 12, lines 4-10 and column 12, lines 40-45). **Dyke** discloses

processing DES algorithm but does not explicitly disclose processing various encryption

algorithms. **Bakhle et al** in an analogous art discloses an input/output module including a

microcontroller and memory (see figure 1), a first encryption sub-module, dedicated to the

processing of symmetric encryption algorithms and being coupled with the first bus of the dual

port memory, for example (see column 5, lines 14-67 and figure 3); a second encryption

sub-module, dedicated to the processing of asymmetric encryption algorithms and being coupled

with a first bus of a dual-port memory and including a separate internal second bus isolated from

the first bus of the dual-port memory, performing parallel processing for example (see column 5,

lines 14-67 and see figure 3). Therefore, it would have been obvious to one of ordinary skill in

the art at the time the invention was made to modify the encryption module of **Dyke** to provide a

first encryption module and second encryption module for simultaneously performing various

encryption algorithms (column 5, lines 14-67) as taught by **Bakhle et al**. This modification

would have been obvious because one skilled in the art would have been motivated by the

suggestions provided by **Bakhle et al** to provide a cryptographic device capable of performing

cryptographic operations in different formats and while one operation is being performed another

can be performed concurrently or in parallel, for instance one cipher processor can operate on

data having a first size whereas another processor can operate on a second block size (column 5,

lines 14-27 and column 1, lines 32-45).

     As per claim 29, Dyke substantially discloses an encryption circuit wherein the

microcontroller comprises an input/output processor and a PCI interface for executing the data

transfers between the host system and the circuit (column 3, lines 55-67; column 4, lines 8-40).

Bakhle et al discloses an encryption circuit wherein a microcontroller comprises: an input/output

processor and a PCI interface and a flash memory; integrating DMA channels responsible for

executing the data transfers between the host system and the circuit, for example (see column 4,

lines 26-67 and column 5, lines 34-44);

a flash memory containing the code of the input/output processor and a PCI interface,

integrating DMA channels responsible for executing the data transfers between the host system

and the circuit, for example (see column 4, lines 26-67); a flash memory containing the code of

the input/output processor , for example (see column 4, lines 38-42); and an SRAM memory that

receives a copy of the contents of the flash memory upon startup of the input/output processor,

for example (see column 4, lines 26-67). **Bakhle et al** discloses instructions in the memory

subsystem for the processors and examples of memory devices and the like that can be

implemented with the I/O module, such examples include DRAM, ROM, VRAM and the like.

Claim 29 is rejected on the same rationale as the rejection of claims 15-17 above.

As per claims 30-31, the combined references disclose the claimed circuit of claim 15.

Dyke discloses a key interface independent of the interface of the link with the host computer

that meets the recitation of a serial link, which is independent of the dedicated PCI bus, said link

adapted to be controlled by the encryption module, for example (see column 3, line 65 through

column 4, line 22). **Dyke** discloses a device capable of preventing linking together of different

files in storage (column 2, lines 6-20). (See also **Bakhle et al,** column 12, line 48 through

column 13, line 10).

As per claim 32, Dyke discloses the limitation of including a card supporting the circuit

(column 3, lines 51-53).

4.   **Claims 18-28 and 33-34** are rejected under 35 U.S.C. 103(a) as being unpatentable over

US Patent 5,063,596 to **Dyke** in view of US Patent 6,021,201 to **Bakhle et al** as applied to

claims 15-17 and further in view of IBM Technical Disclosure Bulletin, Cryptographic

Microcode Loading Controller for Secure Function, September 1991, NB910934, Pages 1-5.

        As per claims 18-20 and 27-28, both references disclose the claimed encryption circuit

of claims 15-17 and **Bakhle et al** further discloses a first encryption sub-module, dedicated to the

processing of symmetric encryption algorithms and being coupled with the first bus of the dual

port memory, for example (see column 5, lines 14-67 and figure 3); a second encryption

sub-module, dedicated to the processing of asymmetric encryption algorithms and being coupled

with a first bus of a dual-port memory and including a separate internal second bus isolated from

the first bus of the dual-port memory, performing parallel processing for example (see column 5,

lines 14-67 and see figure 3). **Dyke** also discloses encryption circuit comprises of PROM and

SRAM (column 5, lines 1-15). Neither of the references explicitly discloses a using a CMOS

memory which is coupled with the dual-port memory (4) via the first bus of the dual-port

memory containing the encryption keys, for example (see column 6, lines 5-21), which is well

known in the art. These elements are well known in the art in a security device and can be

implemented by the invention disclosed in the reference as mentioned above. IBM Technical

Disclosure Bulletin supports well known art by disclosing a single-chip microcontroller

comprising flash memory, data RAM memory, CMOS memory; the flash memory. This bulletin

further uses a CMOS memory to store security keys because it has the advantage to make

probing and examination more difficult in attempt of removal as the CMOS's is sensitive to light

and static charge. In addition the RAMs could be backed with a battery when the system was

unpowered. Therefore, it would have been obvious to one of ordinary skill in the art of computer

security at the time the invention as combined above to modify the circuit of **Bakhle et al.** to

provide an additional flash memory in the second encryption sub-module and a CMOS memory

coupled with the dual-port memory via the first bus of the dual-port memory containing the

encryption keys as taught in IBM Technical Disclosure Bulletin. This modification would have

been obvious because one skilled in the art would have been motivated to do so in order to make

probing and examination more difficult in attempt of removal and the other advantage would be

that the RAMs could be backed with a battery when the system was unpowered.

As per claim 21, Bakhle et al. discloses the limitation of an encryption circuit

characterized in that the first encryption sub-module comprises an encryption component

coupled with the dual-port memory via the first bus of the memory, comprising various

encryption automata, respectively dedicated to the processing of symmetric encryption

algorithms, and in that the second encryption sub-module comprises at least two encryption

processors, respectively dedicated to the processing of asymmetric encryption algorithms,

coupled with the encryption module via the internal second bus of the second sub-module, for

example (see column 5, lines 14-67 and see figures 3 and 6 with description); and discloses a

control unit comprises a security unit that control input and output and use buses separating from

the dual port bus (see figures 3-6 with description and table 2, column 8; column 13, lines 10 et

seq.) that meets the recitation of and a bus isolator for isolating the second bus from the first bus

of the dual port memory. **Bakhle et al** discloses that the cipher and the hash unit can be

implemented with specific dedicated hardware components known in the art for processing of

asymmetric and symmetric algorithms (see end of column 5). **Dyke** teaches isolating means for

making keys inaccessible to the host system and isolating means for performing parallel

processing (column 12, lines 5-45). Therefore, claim 21 is rejected on the same rationale as the

rejection of claims 15-17 above.

       As per claims 22-23, and 25, Bakhle et al. discloses the limitation of an encryption

circuit characterized in that one of the two encryption processors is of the CIP type, and in that

the other of the two encryption processors is of the ACE type, for example (see column 5, lines

50-67). **Bakhle et al.** discloses that the cipher and the hash unit can be implemented with

specific dedicated hardware components known in the art for processing of asymmetric and

symmetric algorithms (see end of column 5). Having both processors CIP type is a design

choice. Therefore, these claims are rejected on the same rationale as the rejection of claims 15-

17 above.

       As per claims 24 and 26, Bakhle et al. does not explicitly disclose that one of the

processors and the encryption component comprise a FPGA. **Bakhle et al.** discloses input

output buffer arrays, for example (see column 9, lines 55 et seq.) and also discloses that the

cipher and the hash unit can be implemented with specific dedicated hardware components

known in the art for processing of asymmetric and symmetric algorithms (see end of column 5).

It is apparent to one skilled in the art that the units disclosed by **Bakhle et al.** can comprise

FPGA without departing from the spirit and scope of the invention as such unit and component

are also well known in the art. Therefore, these claims are rejected on the same rationale as the

rejection of claims 15-17 above.

As per claims 33-34, Dyke discloses the limitation of including a card supporting the

circuit (column 3, lines 51-53).

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from

the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the

mailing date of this final action and the advisory action is not mailed until after the end of the

THREE-MONTH shortened statutory period, then the shortened statutory period will expire on

the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be

calculated from the mailing date of the advisory action. In no event, however, will the statutory

period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure as the first art discloses parallel processing system and method and the second art

discloses manipulation of processing operations by an agent connected to dedicated memory.

The other arts disclose encryption processor performing cryptographic operations in parallel.

US Patents: 6,079,008 Clery, III; 6,357,004 Davis; 6,434,699 Jones et al; 6,169,700 Luo;
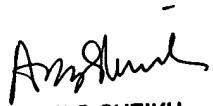
5,333,198 Houlberg et al.

5.2   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The

examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Carl Colin
Patent Examiner
November 23, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100